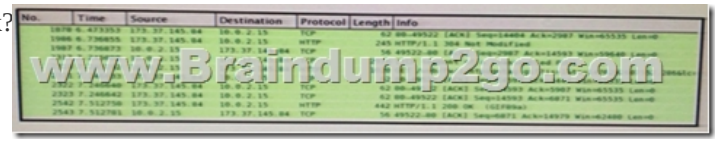
[Dec-2017-NewBraindump2go 210-255 Free VCE Dumps Download[Q26-Q36

2017 New Cisco 210-255 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 210-255 Exam Questions: 1.|2017 New 210-255 Exam Dumps (PDF & VCE) 85Q&As Download: https://www.braindump2go.com/210-255.html2.|2017 New 210-255 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharingQUESTION 26Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?A. confidentialityB. integrityC. availabilityD. complexityAnswer: BQUESTION 27During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?A. collectionB. examinationC. reportingD. investigationAnswer: AQUESTION 28Which information must be left out of a final incident report? A. server hardware configurationsB. exploit or vulnerability usedC. impact and/or the financial lossD. how the incident was detectedAnswer: AQUESTION 29Which two components are included in a 5-tuple? (Choose two.)A. port numberB. destination IP addressC. data packetD. user nameE. host logsAnswer: ABQUESTION 30In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model'?A. victim demographics, incident description, incident details, discovery & responseB. victim demographics, incident details, indicators of compromise, impact assessmentC. actors, attributes, impact, remediationD. actors, actions, assets, attributesAnswer: DQUESTION 31Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?



A. 1986B. 2318C. 2542D. 2317Answer: CQUESTION 32Which two options can be used by a threat actor to determine the role of a server? (Choose two.)A. PCAPB. tracertC. running processesD. hard drive configurationE. applicationsAnswer: CEQUESTION 33Which option creates a display filter on Wireshark on a host IP address or name?A. ip.address == <address> or ip.network == <network>B. [tcp|udp] ip.[src|dst] port <port>C. ip.addr == <addr> or ip.name == <name>D. ip.addr == <addr> or ip.host == <host>Answer: DQUESTION 34You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicous code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4O0) Gecko/20100101D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16Answer: AQUESTION 35A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Diamond Model of Intrusion does this activity fall under?A. reconnaissanceB. weaponizationC. deliveryD. installationAnswer: CQUESTION 36Refer to the Exhibit. A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website?

A. The server at 10.33.1.5 is using up too much bandwidth causing a denial- of-service.B. The server at 10.67.10.5 has a virus. C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors.Answer: C!!! RECOMMEND!!!1.|2017 New 210-255 Exam Dumps (PDF & VCE) 85Q&As Download:https://www.braindump2go.com/210-255.html2.|2017 New 210-255 Study Guide Video: YouTube Video: YouTube.com/watch?v=zDNlMgoc1zI